EXHIBIT 14

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL., **Plaintiffs** **v.** **BRIAN KEMP, ET AL.,** **Defendants.**	**Civil Action No. 1:17-CV-2989-AT**

DECLARATION OF LOGAN LAMB

LOGAN LAMB hereby declares as follows:

1. I am a cybersecurity researcher based in Atlanta, Georgia.

2. I have a Bachelor of Science degree and a Master of Science in computer engineering from University of Tennessee, Knoxville.

3. I have worked professionally in cybersecurity since 2010 where I started at Oak Ridge National Lab in the Cyber and Information Security Research group. In that position, I specialized in static and symbolic analysis of binaries, red-teaming prototype critical infrastructure, and de-identifying geospatial data.

4. I left that operation in 2014 and joined Bastille Networks, a local cyber-security startup business where I am still employed. At Bastille Networks I specialize in wireless security and applications of software defined radio.

DREs are not and will never be secure

5. A DRE (direct-recording electronic) is a voting machine which records votes electronically. DREs do not have a voter-verified paper audit trail, meaning there

is no way of auditing the results of an election. A voter-verified paper audit trail allows voters to independently verify that their vote is being recorded as intended, which is impossible with DREs since the sole record is an electronic copy, and the voter cannot determine how his vote was recorded. Since the only copy of the electronic vote is stored on the machine, there is no way to independently verify the votes cast by voters. If an ostensible audit were to be conducted on DREs, at best this audit would verify the DREs are functioning in a deterministic manner (benign or malicious) at the moment it is being tested. At worst, if the audit results differ from the original then the machines are not functioning in a deterministic manner and the results of the election cannot be trusted, and, unlike paper ballot elections, such errors cannot be remedied.

6. This inherent design flaw, the lack of a voter verified paper trail, means if there are any flaws in how the paperless DRE records votes, then there is no way to detect or correct any mistakes during a post-election audit.

My experience with Diebold voting machines

7. In my research with Diebold AccuVote TS and TSx machines, (the DRE models used in Georgia) I rely on a wealth of academic research conducted detailing how Diebold voting machines have never been a secure way of recording votes, and have known vulnerabilities which call into question results.

8. Motivated by Kohno et al., TTRB, and EVEREST, (see Bernhard Declaration, *passim*) I have begun writing software to independently verify a selection of vulnerabilities of the Diebold AccuVote voting system detailed in those studies. My focus has been on developing methods to quickly verify that the version of software currently used in Georgia, Ballot Station 4.5.2!, is vulnerable to known attacks identified in the academic research. If 4.5.2! is found to be vulnerable to these select attacks, then

it is highly likely that Georgia's version of software is also vulnerable to other attacks detailed in the academic research.

9. Even without running this software to verify likely vulnerabilities affecting version 4.5.2!, the software should be assumed to have critical vulnerabilities since other version of software including 4.3, 4.6, and 4.7 (released before and after 4.5.2!) have had critical vulnerabilities affecting them.

10. I have written software to decrypt ballot results files for BallotStation 4.3.15 and see how votes were cast in order, violating voters' secret ballot protections. I have also created smart-cards which can record the *Smart Card Key* as detailed in EVEREST report (13.3.7). This is the first step in creating illegitimate supervisor cards and infinite voter cards, permitting an unlimited number of votes to be cast by the voter. This vulnerability almost certainly affects 4.5.2! since it affects versions created before and after the Georgia version. I've also written software which is capable of decrypting the file *bs-security.cf* (EVEREST 13.3.5). EVEREST says this attack, "creates the potential for more serious attacks. For instance, malicious software (i.e., a virus) could use this knowledge to alter election results, erase system logs and/or leak the keys necessary to create fraudulent smart cards (e.g., Voter Cards)."

KSU server findings and implications

11. On August 23, 2016 I went to the Fulton County Elections Department in an attempt to meet the Fulton County election supervisor Richard Barron with the hope of gaining access to voting systems equipment so that I could conduct a wireless security assessment as a research project. There I was told to contact Merle King at Kennesaw State University because all election equipment was at that time managed by the Center for Election Systems at KSU.

12. On August 24, 2016 I intended to contact Merle King. Prior to doing so, I wanted to check the CES public website to see if there were any public documents that could give me background on CES and Merle King's duties. I used the search "site:elections.kennesaw.edu inurl:pdf" at www.google.com and discovered what appeared to be files relating to voter registration cached by google.

13. When a search engine like Google caches a file, the search engine makes a local copy of the file in case the original link to the file becomes unavailable. Google had already made copies of some of these files on the CES server prior to my accessing them. So, even if CES were to rectify the situation and remove the files from its web server, Google would still have a copy, generally making it available to the public without authorization

14. After this discovery, I wrote a quick script (simple program) to download what public files were available from the CES server here: https://elections.kennesaw.edu/sites/ , at the time a publicly accessible site. No passwords or authentication were required to gain access to these sensitive files. After running the script to completion, I had acquired multiple gigabytes of data. This data was comprised of many different files and formats, but among them were:

a. voter registration databases filled with personally identifiable information of over six million voters (filename *PollData.db3*). The data included driver's license numbers, birthdates, full home addresses, the last four digits of social security numbers, and more.

b. Election Management System GEMs databases (.gbf and .mdb extensions) GEMS is the central tabulator of the voting system, and used to create ballot definitions, program memory cards and tally and store and report all votes when an election closes. I was able to access and download GEMS databases for at least 15 counties. These GEMS databases use poor encryption, allowing third parties to extract usernames and passwords for multiple databases.

c. Multiple training videos, of particular interest *CES-BulkUpdate_Final.mp4*. This video details how to update the voters' list containing private and personal voter information using a file downloaded over the internet from elections.kennesaw.edu. The video details navigating to elections.kennesaw.edu, logging into the website, downloading *PollDataUpdates.db3*, placing this file on a memory card, inserting that card into an ExpressPoll Unit (the electronic pollbook), and finally applying the absentee update to the ExpressPoll unit. It appears the counties Fulton, Cobb, Dekalb, Gwinnett, Forsyth, Chatham, Muscogee, Henry, Columbia, Clayton, and Cherokee download files from elections.kennesaw.edu and put those files on ExpressPoll units for use in the polling places to validate voters and issue electronic ballots. (I have attached as Exhibits 1 and 2 are collections of documents that I understand were produced by KSU in 2017 in response to an Open Records Act Request. The records referred to in this paragraph appear on Exhibit 1, page 27).

d. PDFs of election day supervisor passwords, for example, *July 2016 Primary and NP Election Runoff Password Memo.pdf.* Supervisor passwords control the administration of the DRE voting machines in the polling place including opening and closing of the voting machines as well as making administrative corrections when machine problems are encountered.

e. Windows executables and DLLs, for example:

- *System.Data.SQLite.DLL*
- *ExpDbCreate.exe*
- *ExpReport.exe*

15. It appears these files are used by the Diebold ExpressPoll (electronic pollbook) units. Since ExpressPoll units are specialized Windows PCs, an attacker can modify theses files and affect the behavior of the ExpressPoll units at the polling place when voters are checked in to vote, assigned a particular ballot style, and approved for voting. A list of vulnerabilities affecting ExpressPoll units is located on the internet at the following URL: https://github.com/josephlhall/dc25-votingvillage-report/blob/master/notes-from-folks-redact.md

16. On August 28, 2016 and August 29, 2016, I contacted King by email and telephone to warn him that CES should assume that the sensitive documents hosted on the "elections.kennesaw.edu" server had already been downloaded by unauthorized persons. Yet for reasons that have never been explained, the server was not secured for months. Along with my colleague Christopher Grayson, I accessed the server again several times in late February 2017 and was able to access and download the same types of files that I had accessed months earlier.

17. Besides making the above information available to the public, the server at elections.kennesaw.edu ("Election Server") was running a version of Drupal, a widely-used content-management framework for websites, which is vulnerable to an exploit called "drupageddon." Using drupageddon, an attacker can compromise a vulnerable server with ease. A public advisory for drupageddon was released in 2014, alerting users that an attack, "can lead to privilege escalation, arbitrary PHP execution, or other

attacks." In practice this means an attacker could have created, modified, or deleted files on the web server, likely without detection.

18. Drupal assigned this vulnerability the highest security risk score possible, 25/25 (Highly Critical).

19. Drupal released a tool to help with the identification of vulnerable servers, called Drupalgeddon (with an L), and made the following critical warning regarding the use of the tool:

> "Drupalgeddon drush command is only useful when restoring from backups is not an option and sufficient expertise is available to attempt a labourious manual recovery. Even then, **neither Drupalgeddon nor an expert can guarantee a website has not been compromised.** They can only confirm with certainty that a site *has* been compromised. This is because:
>
> - Drupageddon attacks may not leave any trace at all
> - Attacks that do leave traces change faster than what Drupalgeddon maintainers can keep up with
> - It is impossible to think of all the places that attackers might hide a backdoor.
> - **There are known exploits that Drupalgeddon does not yet check for.** Contributions are welcome (see below).
>
> If you decide to use Drupalgeddon; **Good luck to you; You will need it.**"

20. Based on internal CES staff emails obtained in public records, management was fully aware of the severity of these vulnerabilities, noting that elections.kennesaw.edu was identified as having "a number of critical and severe vulnerabilities some of which are reported to be exploitable" in September 2016 and "40+ critical vulnerabilities" in October 2016. (The documents referred to in this paragraph may be found on pages 40 and 34 of Exhibit 2.) The fact that the server was allowed to remain online for months until notified again of vulnerabilities is completely inexcusable in my opinion.

21. It is my opinion that the Diebold DRE-based election system and its components should not be used in a public election. It is my opinion that the system, given the level of exposure it was and is still presented with, must be assumed compromised, which necessitates a thorough scrubbing of every component and reinstallation of vendor's certified software. Even after a thorough scrubbing of every component, without software updates to remedy vulnerabilities the risk of compromise and implantation of malware still remains high.

22. From the training video *CES-BulkUpdate_Final.mp4* and open records, we know files from the internet-accessible website elections.kennesaw.edu, a vulnerable server, are placed on ExpressPoll units. This means an attacker could have had a straightforward attack-chain of remotely compromising elections.kennesaw.edu and implanting malware on files that are placed on ExpressPoll units, directly compromising the purportedly "air-gapped" system. Although this particular server no longer operates in the state's election administrative operation, any malware that may have been introduced during periods of security failure would very likely still be present on ExpressPoll books or on the other voting system components which remain in use across the state.

23. The system is flawed by design and made worse by the KSU exposure in ways that cannot be practically mitigated. The system should be treated as untrustworthy for the conduct of Georgia's elections.

Poor Physical Security Affecting Voting Systems

24. I have visited the Fulton County Election Preparation Center on multiple occasions, and have been able to freely roam the facility at times. While observing public

logic and accuracy pre-election testing of voting machines with colleagues, on one such visit I noted:

a. A stack of unsecured supervisor cards, which operate the DRE voting machines;

b. Multiple unsecured voter access cards, which are used by voters to activate their electronic ballot on the DRE;

c. A box of unsecured DRE memory cards;

d. A paper printout of a supervisor password;

e. Multiple unsecured Accuvote TS machines with the hinged door which protects the memory card slot unlocked. (These machines were also powered on. An attacker could have easily inserted a malicious smart card or memory card into these machines.); and

f. The cameras on the interior of the building do not have full view of the facility, an attacker can easily gain access to machines while out of view of the cameras.

An attacker could have easily stolen or modified the various unsecured pieces of election hardware.

25. On July 24th, 2018 my colleagues and I observed the closing of the polls at Grady High School. After the polls were closed, my colleagues and I were left unattended for the evening with the voting machines in the school gymnasium. The only measures taken to secure these voting machines were:

a. A cable lock binding all the voting machines together;

b. Tamper evident seals on the machines; and

c. A single security camera.

26. An attacker could have easily disabled the security camera and then modified or stolen the voting machines. The machines were secured with tamper evident seals which can be purchased on the internet at the following URL: http://www.intab.net/Large-Pull-Tite-Seals/productinfo/03-1330/003%20BLUE/

Summary

27. Based on my personal observations, research and knowledge of the authoritative academic studies, it is my opinion that the use of the Diebold DRE voting machines should be immediately curtailed, and not permitted for use in Georgia's elections. Remaining components of the Diebold DRE-based voting system such as the GEMS server, AccuVote optical scanners, and the ExpressVote electronic pollbooks must undergo decontamination procedures prior to use in future elections.

I declare under penalty of perjury, in accordance with 28 U.S.C. § 1746, that the foregoing is true and correct.

Executed on this date, August 3, 2018.

Logan Lamb